

Please be aware, however, that neither the fact that such use is permitted, nor that you have segregated and labeled this information creates any expectation of privacy or diminishes Neustar's right to monitor, access, use, and disclose personal data and/or communications for a Legitimate Business Purpose.

### **7.3 No Personal Commercial Use**

You may not use Neustar's IT Resources or Confidential Information for non-Neustar commercial or business purposes.

## **8**

Security-Related Information

### **8.1** Security-Related Information

Security-Related Information

Se

### **8.2** Security-Related Information

Security-Related Information

### **8.3 Security-Related Information** Security-Related Information

#### **8.3.1 Security-Related Information**

- Security-Related Information

- Security-Related Information

- Security-Related Information

- Security-Related Information

- Security-Related Information

- Security-Related Information

- Security-Related Information

**8.3.2** Security-Related Information

- Security-Related Information

- Security-Related Information

- Security-Related Information

- Security-Related Information

**8.3.3** Security-Related Information

Security-Related Information

- Security-Related Information

- Security-Related Information

- Security-Related Information

- Security-Related Information

**8.3.4** Security-Related Information

Security-Related Information

Security-Related Information

## **9 Email, Instant Messaging, Telephone and other Electronic Communications Channels**

### **9.1 General Requirements**

Neustar provides several technologies including email, instant messaging, and other technologies supporting communication and collaboration between internal and external (collectively, "Electronic Communications Channels"). The following provisions apply to your use of any such technologies:

- Electronic Communications containing Confidential Information are permanent business records. They are subject to the Neustar Records Management, Retention, and Disposal Policy, and should be treated as a formal, written document. Apply the same standards regarding appropriateness, security, confidentiality, retention and destruction as you would with similar Neustar records.
- Use only Neustar provided or approved Electronic Communications Channels to conduct Neustar business.
- Do not use Neustar-provided Electronic Communications Channels to:
  - Distribute information that is inconsistent with Neustar policy, contrary to Neustar's interests, or in violation of applicable law;
  - View, intentionally receive, download, or distribute foul, obscene, sexually explicit, harassing or otherwise inappropriate information or content;
  - Distribute information, applications, or content of any type that violates another's rights in copyrighted, trademarked, proprietary and/or trade secret materials, including downloading, sending, or copying materials, files, etc. in violation of any applicable Terms of Usage or license;
  - Create, copy, transmit, or retransmit unauthorized mass mailings, regardless of the subject matter;
  - Distribute non-Neustar advertisements or solicitations; or
  - Distribute information that is obtained or used for personal gain (e.g., non-Neustar for-profit business affairs).

### **9.2 Right to Access**

To the extent permitted by applicable law, Neustar reserves the right to block access to, audit, monitor, access, record, and disclose any Electronic Information and/or Electronic Communications created, received, sent, or stored on Neustar IT Resources or on Personal Devices used to access IT Resources or Confidential Information for a Legitimate Business Purpose.

### **9.3 No Expectation of Privacy**

You may have no expectation of privacy in any Electronic Information or Electronic Communications created, stored, or transmitted using Neustar IT Resources. Your expectation of privacy with respect to Electronic Information and Electronic Communications created, stored, or transmitted via Personal Devices used to access Confidential Information and/or IT Resources is limited in accordance with the Personal Device User Policy and Agreement.



#### 9.4 Email and Instant Messaging

- Neustar email is provided for business purposes only. While Neustar permits limited personal use of Neustar IT Resources to access and send personal email using a web mail service, Neustar strongly discourage use of Neustar email for personal communications.
- Security-Related Information
  - Use only Neustar-provided or approved Personal Devices and remote access services to access Neustar IT Resources, including to access your Neustar email account and/or to transmit Confidential Information when working remotely.
  - Do not respond to unsolicited or junk electronic communications ("spam").
  - Use caution when opening an email from an unknown or unsolicited source and never open an email attachment from an unknown or unsolicited source. If you have received an email that looks suspicious but still needs to be reviewed, contact the NeuCIRT (email [Neucirt@neustar.biz](mailto:Neucirt@neustar.biz) or call 1-855-638-2478).
  - Do not respond to unsolicited email inquiries or requests unless you know the sender or have confirmed that the user is associated with a reputable institution, organization, or company doing business with or know to Neustar.
  - Do not use personal email or webmail accounts to send Confidential Information as email attachments. If you must temporarily send a Neustar email to your personal email account to meet a critical business requirement, delete the email and any attachments or downloads promptly once you are done.
  - Never disguise your identity in Electronic Communications or distribute anonymous email messages using a Neustar-provided Electronic Communication Channel.
  - Do not use instant messaging to transmit Confidential Information, including Sensitive Personal Information.

#### 9.5 Telephone

- To the extent permitted by applicable law, Neustar may monitor and/or record telephone conversations for Legitimate Business Purposes.
- Do not use online telephone services such as Skype to conduct sensitive Neustar business and/or to transfer Sensitive Personal Information or other highly sensitive Confidential Information.

### 10 Internet Usage and Use of Other Electronic Communications Channels

Your use of the Internet using Neustar equipment or through a Neustar Network is subject to this policy.

- Neustar provides Internet access for business purposes. Limited personal use of the internet in compliance with Section 7 of this Policy is permitted.
- Never post Confidential Information without specific authorization to any public Internet site, including but not limited to public email sites, social media sites, Blogs, Wikis, message boards, and newsgroups.

- Never download materials from the Internet in response to a prompt from an unknown or unsolicited source.
- Use a personal email address when registering with non-work related public Internet sites.
- Do not use public Internet services, including public mail sites such as Hotmail or gmail, to distribute, share, or comment on Neustar or to share Neustar Confidential Information.
- Do not download or install peer-to-peer file sharing software, such as Napster or Limewire, without IT's (Infrastructure Services) written authorization.
- Do not use the Neustar IT Resources, including Neustar-provided web browsers, to send, display, download or print potentially offensive messages, pornographic or sexually explicit pictures, or derogatory religious or racial materials.
- Do not use public Internet sites (including but not limited to public email sites, social media sites, message boards, newsgroups etc.) to conduct Neustar business without the consent of the Senior Vice President in your business unit and the General Counsel.
- Do not use or create unauthorized list serves or distribute unauthorized newsletters or marketing materials via the Internet.

## 11 Social Media Usage

Social media and online community services such as Facebook, LinkedIn, and Twitter are increasingly popular. These services can be leveraged for the benefit of Neustar; for example Neustar has a presence on Facebook and LinkedIn for recruiting and information-sharing purposes.

- Adhere to all policies and guidelines stated in the Neustar Social Media Guidelines when using Neustar and non-Neustar IT Resources to participate in social media communities and activities.
- Neustar permits limited and occasional use of its Information Resources for personal blogging, provided that it does not impact your job performance or violate Neustar policy, including the *Neustar Social Media Guidelines*.

## 12 Remote Access

- You are responsible for safeguarding Confidential Information and IT Resources when working remotely, in compliance with Neustar's Remote Access Policy.
- Neustar provides remote technologies to access IT Resources and Confidential Information when off-site. You are permitted to access these services using Neustar Equipment or approved Personal Devices only. Do not attempt to access Neustar IT Resources using any method other than Neustar provided remote access services.
- Unless absolutely necessary, do not use Neustar remote access services from public computers such as those located in airport kiosks.
- Security-Related Information
- For additional information regarding Neustar's remote access connection options, including how to order or disconnect service, cost comparisons, and troubleshoot, contact the Helpdesk.



### 13 Use of Mobile Devices

- You are expected to exercise reasonable care to safeguard any Neustar-provided mobile device or Personal Device used to access Neustar IT Resources in accordance with Neustar's Mobile Computing Policy. Treat the device with the same level of care and concern as you do your wallet, purse or passport, and keep track of its whereabouts at all times.
- You may use IT-approved personal mobile devices, subject to central configuration and management requirements, in accordance with Neustar's Personal Device User Policy and Agreement.
- Do not store sensitive Confidential Information, including Sensitive Personal Information on mobile devices, including Personal Devices unless they have been protected using Neustar-approved encryption technology.
- You must install and maintain Neustar-approved anti-virus and malware and personal firewalls on mobile devices used to access or store Confidential Information.
- Use passwords that comply with the Neustar Password Policy, and do not permit others – including family members – to access Confidential Information on any portable device.
- In accordance with the Personal Device User Policy and Agreement, Neustar has the right to install security-related software on Personal Devices used to access Neustar IT Resources and/or Confidential Information, and reserves the right to access and monitor the use of Personal Devices for Legitimate Business Purposes.
- Report lost or stolen mobile devices, including Personal Devices, used to access Neustar IT Resources to the NeuCIRT (email [Neucirt@neustar.biz](mailto:Neucirt@neustar.biz) or call 1-855-638-2478) promptly.

### 14 Neustar Equipment

#### 14.1 General

- You are responsible for safeguarding Neustar Equipment in your possession.
- You must return all Neustar Equipment in your possession or control in good working order upon separation from the company, when you no longer need it to perform your employment responsibilities, or at the request of your supervisor or manager. You may be required to reimburse Neustar for the cost of replacing Equipment that is not returned in a timely fashion.
- Neustar's maintenance policies cover mechanical breakdown and theft of Neustar Equipment. Recognizing that accidents do happen, Neustar generally will not charge you for the cost of repairing or replacing Neustar Equipment. Neustar reserves the right, however, to hold you responsible for repeated, excessive, or unusually frequent incidents resulting in repair or replacement costs.

#### 14.2 Laptops and Desktops

- Users are not granted administrator rights on desktops or laptops. You may not download or install applications and/or software without the approval of IT (Infrastructure Services). Certain updates are set to install automatically (e.g., Windows patches and updates). In all other cases, the Helpdesk will assist you in installing approved applications, operating systems and updates on all Neustar Equipment.

- You may not store large personal files, including videos, music, or movie files on Neustar Equipment.
- To the extent permitted by applicable law, Neustar reserves the right to access, record, image, delete, or copy electronic content and/or information stored on computers used to access Neustar IT Resources and/or Confidential Information for Legitimate Business Purposes.
- **Security-Related Information**
- You may not interfere with Neustar efforts to synchronize files to server disks during login and logoff.
- Inform the NeuCIRT (email [Neucirt@neustar.biz](mailto:Neucirt@neustar.biz) or call 1-855-638-2478) immediately if virus scanning software detects a virus on your computer.
- You may not, under any circumstances, copy or transmit Neustar-provided software and/or applications.

#### **14.3 Physical Security of Laptops and Desktops.**

- Secure your laptop and all portable computing devices when unattended.
- Keep your Neustar laptop in your physical possession at all times and within sight when you are outside of Neustar premises.
- Report lost or stolen Neustar-provided or personal laptops and computers used to access Neustar IT Resources to the NeuCIRT (email [Neucirt@neustar.biz](mailto:Neucirt@neustar.biz) or call 1-855-638-2478) promptly.

### **15 Clear Desk and Clear Screen**

- Secure Confidential Information, whether in hard copy or on electronic media, when unattended and/or not in active use.
- Log off or screen-lock your computer when it is not in active use to protect the confidentiality and security of information on your screen (note: Neustar PC screens will automatically lock after a specified period of inactivity).
- Promptly retrieve documents containing Confidential Information from printers, copiers, fax machines, or other reproduction systems.
- Neustar permits the limited, incidental, and non-commercial personal use of Neustar photocopiers, fax machines, etc.

## **16 Enforcement**

You are subject to disciplinary action for any violation of this Policy, up to and including termination of employment.

## **17 Exemptions**


You may request an exemption from any part of this Policy, supported by a comprehensive and detailed business justification. Any exemption granted must be approved by the General Counsel and limited to the specific scenario for which it was granted.

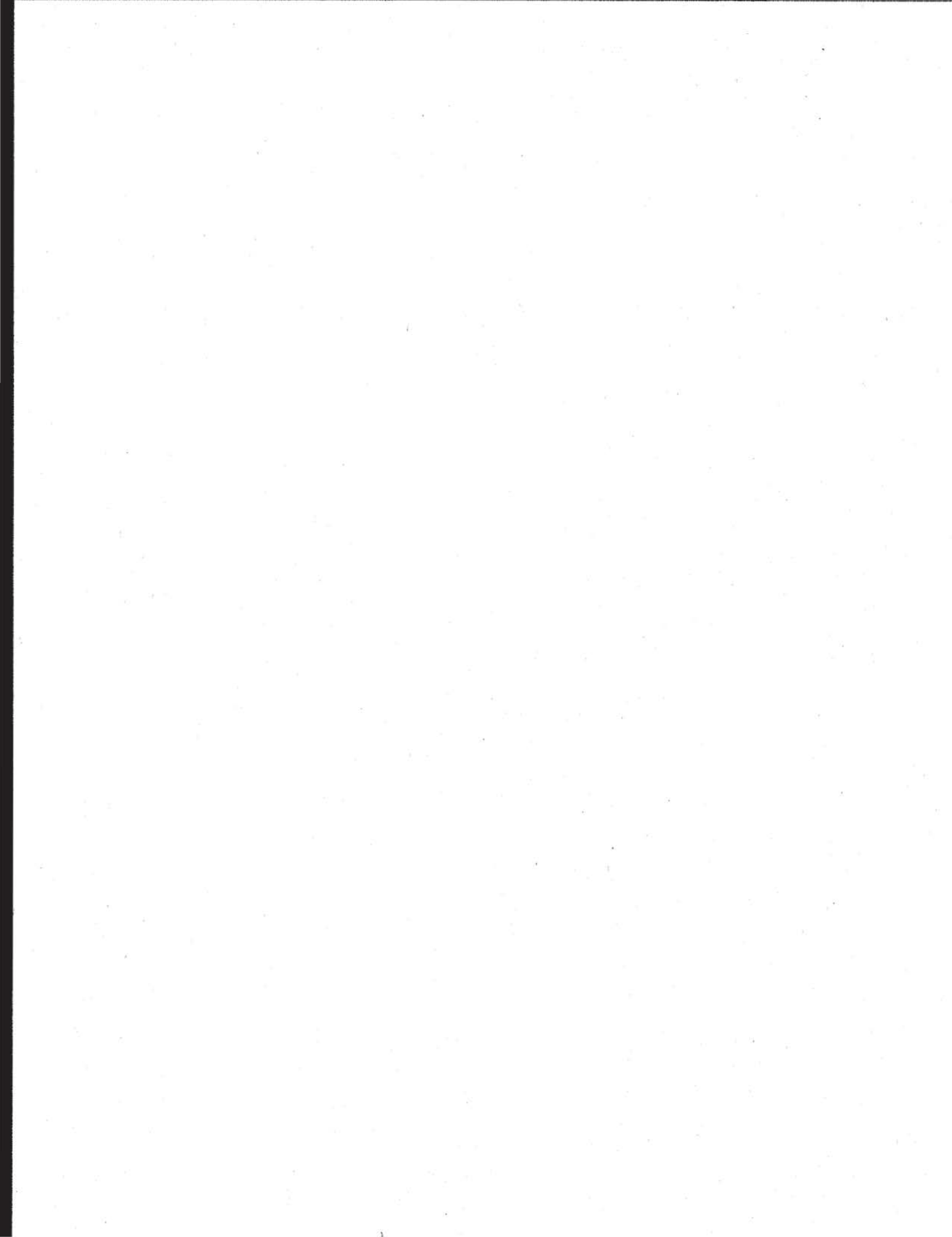
## **18 Revisions**

This policy will be re-evaluated, modified, and re-issued periodically to ensure compliance with changing requirements and industry standards. Updates and revised policies become effective upon release.



## Appendix A: Document Control

		Doc Title:	Acceptable Use of Technology Resources Policy
		Doc Revision:	2.2
<b>Revision Control</b>			
1.0	1/31/2010	Information Security	Initial Release
1.1	5/19/2011	Information Security	Review for 2011
1.2	1/13/2012	Information Security	General Review
2.0	3/1/2013	Legal	Comprehensive Revision
2.1	8/9/2013	Legal	Replaced "helpdesk" with NeuCirt
2.2	9/3/2013	Legal	Added reference to privacy policy principles
<b>Document Approvals of Current Revision</b>			
2.2	Becky Burr	Deputy General Counsel/Chief Privacy Officer	9/3/2013
<b>Send all Questions, Suggestions and Recommendations regarding the content of this document to <a href="mailto:CPO@neustar.biz">CPO@neustar.biz</a>.</b>			
<p>The information contained herein is proprietary to Neustar, Inc. Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited. Limit distribution accordingly. The names, logos, and taglines identifying Neustar's products and services are proprietary marks of Neustar, Inc. All other trademarks and service marks are the property of their respective owners. © Neustar, Inc. 1999-2013</p> <p>Printed copies of this document are uncontrolled and are subject to change without notice. The master copy of this document can be found in Document Management.</p>			



NEUSTAR DATA CLASSIFICATION MATRIX – CONFIDENTIAL UNDER NON-DISCLOSURE AGREEMENT

# Security-Related Information

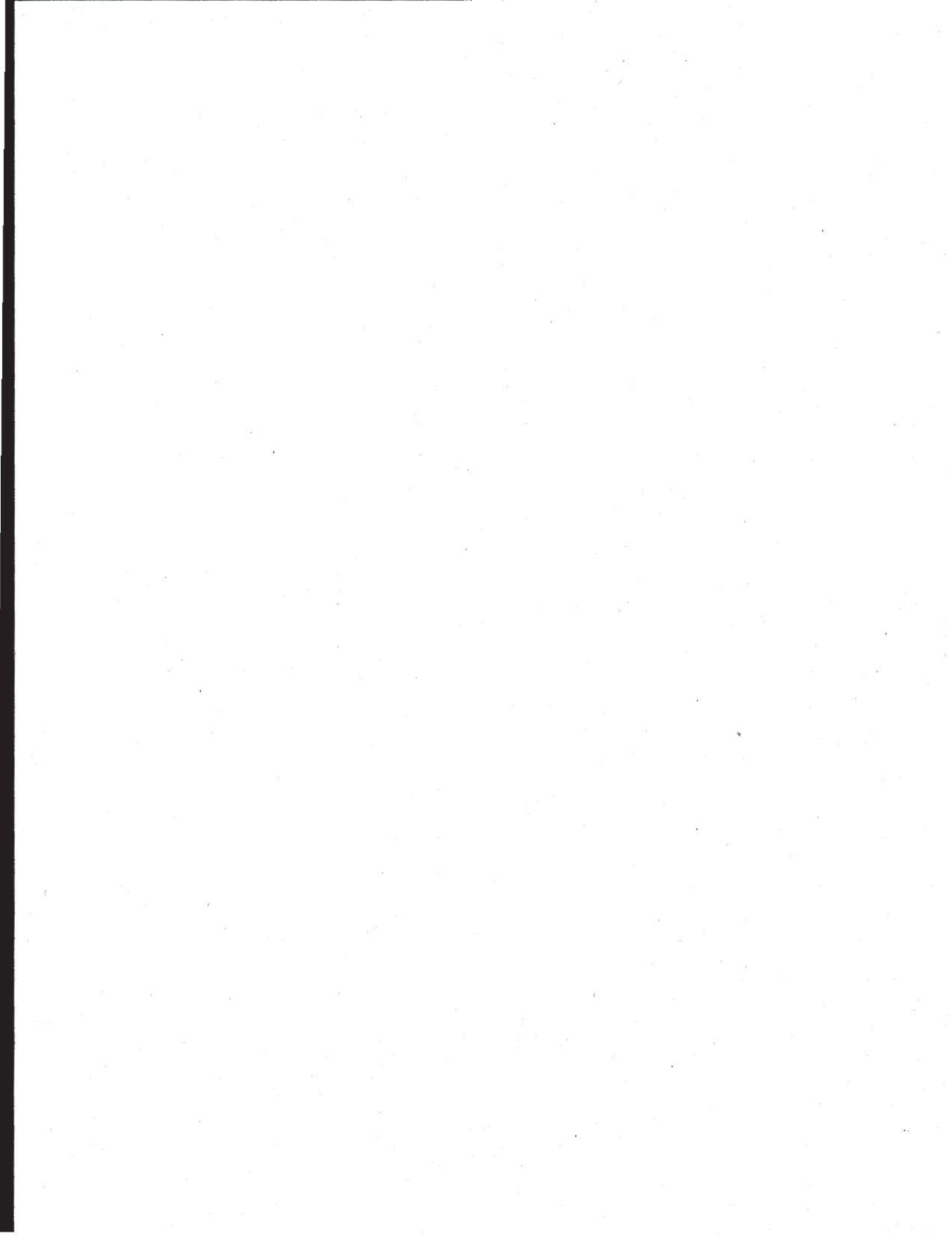


# Security-Related Information

# Security-Related Information

# Security-Related Information





# Neustar Data Classification Policy

## Version 2.0

Effective Date: May 1, 2013

**neustar**<sup>TM</sup>

# Table of Contents

Table of Contents .....	1
1 Purpose .....	2
2 Scope .....	2
3 Definitions .....	2
4 Data Classification .....	3
5 Roles and Responsibilities .....	3
5.1 Information Owners .....	3
5.2 Information Custodians .....	4
5.3 CPO and CISO .....	4
6 Policy .....	4
6.1 Classification of Neustar Information .....	4
6.2 Mixed Category Information .....	4
6.3 Classification Review .....	4
6.4 Controls .....	4
6.5 NeuHub Registration .....	4
7 Enforcement .....	4
8 Revisions .....	4
Appendix A: Document Control .....	5



## **1 Purpose**

This Neustar Data Classification Policy and Matrix, (collectively, the "Policy") is intended to help employees determine the extent to which Neustar's Confidential Information may be disclosed within the company and to third parties, and defines certain safeguards that must be observed to protect different kinds of data.

## **2 Scope**

- The information covered by this policy includes all information that is generated, created, received, possessed, accessed, stored, used or disclosed to accomplish business objectives (as defined below, "Confidential Information"). It applies to Confidential Information in electronic format, email and voice mail, information on paper, and information shared orally or visually (such as telephone and video conferencing).
- Neustar employees, including temporary employees and consultants (collectively, "Employees") who handle Neustar Information in the course of performing their duties are must comply with this Policy. In addition, the Policy applies to clients, customers, vendors, service providers, business partners and any other party with access to Neustar Information (collectively, "Third Parties").
- This Policy supplements but does not replace or eliminate your obligation to comply with relevant provisions of the Neustar Information Security Policy, the Policy on Acceptable Use of Technology Resources, and other policies and procedures issued to safeguard Neustar Information Assets.

## **3 Definitions**

Confidential Information includes all of Neustar's proprietary business information, including, without limitation, the following:

- Information relating to Neustar's planned or existing computer systems and systems architecture, including computer hardware, computer software, source code, object code, documentation, methods of processing and operational methods;
- Information regarding existing, former, or prospective Neustar customers and any information received from such customers or created by Neustar in the course of providing services ("Customer Information");
- Information that identifies or can be used to identify specific individuals including Neustar employees and/or their dependants and beneficiaries, applicants for employment, customers and their subscribers or end users, and others ("Personal Information")
- "Sensitive Personal Information" is a subset of Personal Information consisting of a person's name in combination with an item such as (1) a social security number or other government-issued identifier; (2) a credit card, bank account, or other financial account number; (4) medical, lifestyle, or other highly personal information;
- Business information relating to Neustar and its affiliates including financial information, organizational structure, business initiatives, intellectual property, product plans, design or requirements documents, and strategic or other plans;
- Confidential information of third parties, including Neustar's customers, vendors, suppliers, contractors, partners, and acquisition targets;
- Other confidential and/or proprietary information that Neustar receives, uses, creates, stores, and/or transmits as part of its day-to-day business activities; and

- Any information that someone familiar with Neustar's business would consider confidential or proprietary, the maintenance of which would be important to Neustar, its employees, and/or its customers.

## 4 Data Classification

Neustar Information falls into one of four categories, based on the nature of the data itself, any legal, regulatory, contractual or other limits on our use of the data, and the extent to which unauthorized use or disclosure of the information could harm the company, our investors, employees, customers, or others.

The categories, which are detailed in the Classification Matrix, are summarized below:

- **Restricted Information** includes sensitive corporate, legal, and financial, human resources, client, or personal information that requires a high degree of protection in order to comply with law, regulation, and/or contractual obligations and/or to protect the company, employees, shareholders, customers, or others. Restricted Information is a subset of Proprietary Information.
- **Proprietary Information** is proprietary and/or confidential to Neustar, the disclosure of which outside the company would be inappropriate and/or inconvenient.
- **Internal Use Only Information** is proprietary and/or confidential to Neustar, but intended and approved for wide distribution within the company.
- **Public Information** is information that is intended and approved for public dissemination.

You should use common sense in applying these data classifications. If you are uncertain about the proper classification of a specific piece of information, contact your supervisor, a Data Steward in your business unit (identified below), or the Data Privacy, Security, and Governance Working Group office.

## 5 Roles and Responsibilities

### 5.1 Information Owners

Business units will identify an "Owner" (by name, position, or team) for all Neustar Information. The role of the Owner of specific Neustar Information is to:

- Classify and mark the data in accordance with the Data Classification Matrix;
- Identify Employees and Third Parties authorized to access and use the data;
- Ensure that appropriate controls are in place to enforce applicable marking, access, disclosure, reproduction, storage, transmission, and destruction requirements specified in the Data Classification Matrix
- Register relevant Information in NeuHub; and
- Authorize exceptions to the relevant requirements in consultation with management, the Chief Privacy Officer and the Chief Information Security Officer.



## 5.2 Information Custodians

Employees and Third Parties authorized by the Owner to access and use particular data sets are referred to as “Custodians” of that Information. Custodians are responsible for complying with the requirements specified in the Data Classification Matrix and additional controls specified by the Owner.

## 5.3 CPO and CISO

The Chief Privacy Officer and the Chief Information Security Officer, in consultation with the Information Management Working Group, are responsible for reviewing and, if necessary, revising this policy annually.

# 6 Policy

## 6.1 Classification of Neustar Information

Neustar Information will be classified to the extent possible at the time of collection, creation, or receipt and must be classified prior to distribution and/or disclosure.

## 6.2 Mixed Category Information

Documents or datasets that include both Proprietary and Restricted Information must be treated as Restricted Information unless the restricted elements are hashed or masked.

## 6.3 Classification Review

Neustar Information will be reviewed, and re-classified where necessary, whenever it is incorporated into, associated with, or used in connection with additional data set(s).

## 6.4 Controls

Neustar Information will be marked, accessed, disclosed, reproduced, stored, transmitted, and destroyed in compliance with controls and requirements applicable to its classification, as published from time to time in the Classification Matrix.

## 6.5 NeuHub Registration

Neustar will create and maintain an inventory of datasets (NeuHub), including Customer Information and Licensed Data, used to deliver products and services or created in the course of providing products and services. The registration information will identify Restricted Information at the field or element level.

# 7 Enforcement


Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

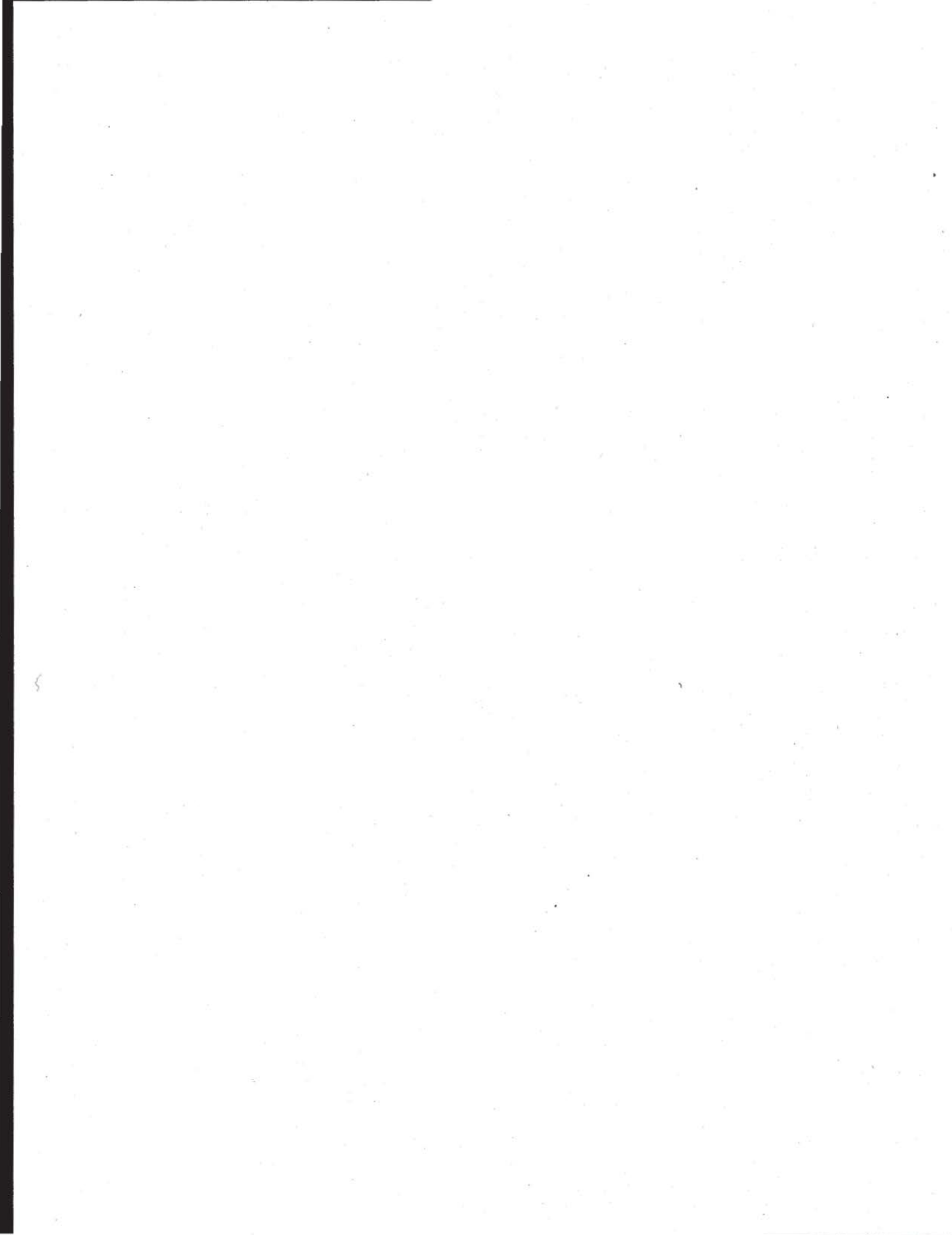
# 8 Revisions

This policy will be re-evaluated, modified, and re-issued periodically to ensure compliance with changing requirements and industry standards. Updates and revised policies become effective upon release.



## Appendix A: Document Control

		Doc Title:	Data Classification Policy
		Doc Revision:	2.0
<b>Revision Control</b>			
2.0	5/1/2013	CONFIDENTIAL	Comprehensive revision and name change
<b>Document Approvals of Current Revision</b>			
2.0	CONFIDENTIAL	Chief Privacy Officer	5/1/2013
2.0	CONFIDENTIAL	Chief Information Security Officer	5/1/2013
<p><b><i>Send all Questions, Suggestions and Recommendations regarding the content of this document to <a href="mailto:CPO@neustar.biz">CPO@neustar.biz</a>.</i></b></p> <p>The information contained herein is proprietary to Neustar, Inc. Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited. Limit distribution accordingly. The names, logos, and taglines identifying Neustar's products and services are proprietary marks of Neustar, Inc. All other trademarks and service marks are the property of their respective owners. © Neustar, Inc. 1999-2013</p> <p>Printed copies of this document are uncontrolled and are subject to change without notice. The master copy of this document can be found in Document Management.</p>			



# Neustar Information Security Policy

## Version 1.1

Effective Date: April 26, 2013

**neustar**<sup>TM</sup>

**Table of Contents**

Table of Contents ..... 1

1 Security-Related Information

## Security-Related Information